

## 参考サイト

### IE8 セキュリティー パート VII: クリックジャッキングを防ぐ / MSDN

・ <http://msdn.microsoft.com/ja-jp/ie/dd560562.aspx>

最善に設計された Web アプリケーションでは、被害者のユーザーが意図的に送信したのではない不正なリクエストを識別できるチャレンジトークン(英語)やそれに類似した手法を使い、自身を保護しています。

残念ながら、チャレンジトークンやそれに類似した手法は脆弱性に陥りやすいのです。第一の脆弱性はクロスサイトスクリプティング(英語)(XSS)です。トークンで保護された Web アプリケーションにクロスサイトスクリプティングの脆弱性があると、セキュリティートークンが盗まれ CSRF 攻撃が可能になります。

機微情報を扱うアンチ CSRF のページを保護するために、X-FRAME-OPTIONS 指示子を使う事で、Web 開発者は IE 8 のユーザーへの web アプリケーションを通じた攻撃をただちに軽減する事ができます。